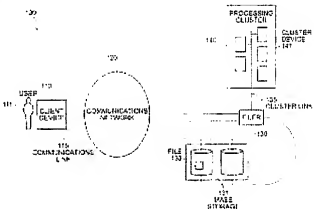
DECENTRALIZED APPLIANCE VIRUS SCANNING

Publication number: JP2004523820 (T)
Publication date: 2004-08-05
Inventor(s):
Applicant(s):
Classification:
- international: ***G06F21/22; G06F7/00; G06F11/00; G06F11/30; G06F11/34; G06F17/30; G06F21/00;*** **G06F21/22; G06F; G06F7/00; G06F11/00; G06F11/30; G06F11/34; G06F17/30; G06F21/00;** (IPC1-7): G06F11/00
- European: G06F21/00N3V4
Application number: JP20020546962T 20011130
Priority number(s): US20000728701 20001201; WO2001US46688 20011130

Also published as:
WO0244862 (A2)
WO0244862 (A3)
US7346928 (B1)
US2002103783 (A1)
WO02095588 (A2)
more >>

Abstract not available for JP 2004523820 (T)
Abstract of corresponding document: **WO 0244862 (A2)**

The invention provides a method and system for scanning specialized computing devices for viruses. In a preferred embodiment, a filer is connected to one or more supplementary computing devices that scan requested files to ensure they are virus free prior to delivery to end users. When an end user requests a file the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one of the external computing devices and sends the filename. Third, the external computing device opens the file and scans it. Fourth, the external computing device notifies the filer the results of the file scan operation. Fifth, the filer sends the file to the end user provided the status indicates it may do so.



Data supplied from the ***esp@cenet*** database — Worldwide

(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-523820
(P2004-523820A)
(43)公表日　平成16年8月5日(2004.8.5)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 11/00	G06F 9/06	660N	5B076

審査請求 未請求　予備審査請求 有　（全 46 頁）

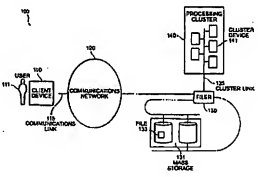
(21)出願番号	特願2002-546962(P2002-546962)
(86)(22)出願日	平成13年11月30日(2001.11.30)
(85)翻訳文提出日	平成15年6月2日(2003.6.2)
(86)国際出願番号	PCT/US2001/046688
(87)国際公開番号	WO2002/044862
(87)国際公開日	平成14年6月6日(2002.6.6)
(31)優先権主張番号	09/728,701
(32)優先日	平成12年12月1日(2000.12.1)
(33)優先権主張国	米国(US)
(81)指定国	EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),CA,JP

(71)出願人　500261341
ネットワーク・アプライアンス・インコーポレイテッド
アメリカ合衆国９４０８９カリフォルニア州サニーベイル、イースト・ジャーバ・ドライブ４９５番
(74)代理人　100086405
弁理士　河宮　治
(74)代理人　100098280
弁理士　石野　正弘
(72)発明者　マーク・ムールスタイン
アメリカ合衆国８５７５０アリゾナ州ツーソン、イースト・プラチタ・アルタ・レボサ５８３１番

Fターム(参考)　5B076 FD08

(54)【発明の名称】分散化された装置でのウィルススキャン

(57)【要約】
特殊なコンピュータ装置をウィルススキャンする方法およびシステムである。好適実施形態にて、ファイラ（１３０）は、エンドユーザへの配信の前にリクエストされたファイルがウィルスフリーであることを確かめる１以上の補助コンピュータ装置（１４０）に接続される。エンドユーザ（１１１）のファイルリクエストにより、以下の工程が実施される。第１に、リクエストファイルをエンドユーザへ送信する前にスキャンしなければならないのか判断する。第２に、ファイラは外部コンピュータ装置の１つ（１４１）へのチャンネルを開き、ファイル名を送る（２０３）。第３に、その外部コンピュータ装置がそのファイルを開いて（２０５）スキャンする（２０７）。第４に、外部コンピュータ装置がファイラへファイルスキャン操作のステータスを報告する（２０９）。第５に、ファイラは、ステータスが送信を許可するならば、ファイルをエンドユーザに送る（２１１）。



【特許請求の範囲】
【請求項１】
ファイラを操作する方法であって、
オブジェクトを有する第１ロケーションにおいて、第１通信リンクを介してユーザからの前記オブジェクトに対するリクエストを受け取るステップ、
前記オブジェクトに関する識別子を、第２通信リンクを介して第２ロケーションに送るステップ、
前記第２ロケーションにおける前記リクエストの処理ステップであって、前記処理のステップに少なくとも以下の、
（１）前記オブジェクト内部において１以上の認識可能なデータパターンを検索すること、
（２）前記オブジェクトを圧縮すること、および、
（３）前記オブジェクトを暗号化すること、
のうち１つを含んでいるステップ、
ならびに、
前記リクエストに対する応答ステップであって、前記応答ステップが前記第１通信リンクを介して前記ユーザに対しレスポンスを送信することを含んでいるステップを有する、
ファイラを操作する方法。
【請求項２】
前記リクエストが電子形式で行われる、請求項１に記載の方法。
【請求項３】
前記オブジェクトがファイルである、請求項１に記載の方法。
【請求項４】
前記リクエストの処理ステップがさらに以下の、
前記ファイラから処理クラスタへのアクセスパスを生成するステップ、
前記処理クラスタにおいて前記ファイルを処理するステップ、および、
前記処理クラスタにおいて前記ファイルに関する前記処理に対応したスキャンレポートを作成するステップを含んでいる請求項３に記載の方法。
【請求項５】
前記アクセスパスを生成するステップが、
前記ファイラから前記処理クラスタへ前記ファイルのＩＤおよびパスを送信するステップを有する請求項４に記載の方法。
【請求項６】
前記送信ステップが不均等メモリアクセスを用いて遂行される請求項５に記載の方法。
【請求項７】
前記送信ステップが通信ネットワークを用いて遂行される請求項５に記載の方法。
【請求項８】
前記送信ステップがダイレクト接続を用いて遂行される請求項５に記載の方法。
【請求項９】
前記の、前記ファイルを処理するステップは、前記処理クラスタにより総当り方式で後続の受信ファイルについて実行される請求項４に記載の方法。
【請求項１０】
前記の、前記ファイルを処理するステップは、前記処理クラスタにおける１よりも多い装置により、分けて遂行される請求項４に記載の方法。
【請求項１１】
前記ファイラに記憶されている全てのファイルは論理的に連続的な方式でスキャンされる請求項４に記載の方法。
【請求項１２】
前記スキャンレポートが、前記の、前記ファイルを処理するステップに関する一組のステータスデータを有する請求項４に記載の方法。

【請求項１３】
前記ステータスデータが、前記ファイルにおけるウィルスの存在または非存在を特定する少なくとも１つのデータ要素を含んでいる請求項１２に記載の方法。
【請求項１４】
前記レポートが前記ファイラへ転送される請求項１３に記載の方法。
【請求項１５】
前記レポートが第１データベースに記憶される請求項１４に記載の方法。
【請求項１６】
その後の、前記ファイルに対するスキャンの必要性は、前記データベースが前記ファイルに関するレポートを有するか、および、前記ファイルが最後のアクセスから変更されているかに関する判断による関数である、請求項１５に記載の方法。
【請求項１７】
その後の、前記ファイルに対するスキャンの必要性は、さらなるウィルス識別データファイルが前記処理クラスタに追加されたかに関する判断による関数である、請求項１６に記載の方法。
【請求項１８】
前記レスポンスの送信とは前記ファイルである請求項１に記載の方法。
【請求項１９】
前記レスポンスの送信が、ユーザへの前記ファイルは利用不可能である旨の通知を含む請求項１に記載の方法。
【請求項２０】
前記リクエストに対する応答ステップが、前記ユーザに前記スキャンレポートの写しを送ることを含んでいる請求項１に記載の方法。
【請求項２１】
ファイラを操作するための装置であって、
オブジェクトを有する第１ロケーションにおいて、第１通信リンクを介してユーザからの前記オブジェクトに対するリクエストを受け取るための手段、
前記オブジェクトに関する識別子を、第２通信リンクを介して第２ロケーションに送るための手段、
前記第２ロケーションにおける前記リクエストの処理のための手段であって、前記処理のための手段に少なくとも以下の、
（１）前記オブジェクト内部において１以上の認識可能なデータパターンを検索するための手段、
（２）前記オブジェクトを圧縮するための手段、および、
（３）前記オブジェクトを暗号化するための手段、
のうち１つを含んでいる手段、
ならびに、
前記リクエストに対する応答手段であって、前記応答手段が前記第１通信リンクを介して前記ユーザに対しレスポンスを送信する機能を備えた手段を有する、
ファイラを操作するための装置。
【請求項２２】
前記オブジェクトがファイルである、請求項２１に記載の装置。
【請求項２３】
前記リクエストの処理のための手段がさらに以下の、
前記ファイラから処理クラスタへのアクセスパスを生成するための手段、
前記処理クラスタにおいて前記ファイルを処理するための手段、および、
前記処理クラスタにおいて前記ファイルに関する前記処理に対応したスキャンレポートを作成するための手段を含んでいる請求項２２に記載の装置。
【請求項２４】
前記アクセスパスを生成するための手段が、

前記ファイラから前記処理クラスタへ前記ファイルのＩＤおよびパスを送信するための手段を有する請求項２３に記載の装置。

【請求項２５】

前記送信が不均等メモリアクセスを用いて遂行される請求項２４に記載の装置。

【請求項２６】

前記送信が通信ネットワークを用いて遂行される請求項２４に記載の装置。

【請求項２７】

前記送信がダイレクト接続を用いて遂行される請求項２４に記載の装置。

【請求項２８】

前記の、前記ファイルに対する処理は、前記処理クラスタにより総当り方式で後続の受信ファイルについて実行される請求項２３に記載の装置。

【請求項２９】

前記の、前記ファイルに対する処理は、前記処理クラスタにおける１よりも多い装置により前記ファイルの極小単位に遂行される請求項２３に記載の装置。

【請求項３０】

前記ファイラに記憶されている全てのファイルは論理的に連続的な方式でスキャンされる請求項２３に記載の装置。

【請求項３１】

前記スキャンレポートが、前記の、前記ファイルに対する処理に関する一組のステータスデータを有する請求項２３に記載の装置。

【請求項３２】

前記ステータスデータが、前記ファイルにおけるウィルスの存在または非存在を特定する少なくとも１つのデータ要素を含んでいる請求項３１に記載の装置。

【請求項３３】

前記レポートが前記ファイラへ転送される請求項３１に記載の装置。

【請求項３４】

前記レポートが第１データベースに記憶される請求項３３に記載の装置。

【請求項３５】

その後の、前記ファイルに対するスキャンの必要性は、前記データベースが前記ファイルに関するレポートを有するか、および、前記ファイルが最後のアクセスから変更されているかに関する判断による関数である、請求項３４に記載の装置。

【請求項３６】

その後の、前記ファイルに対するスキャンの必要性は、さらなるウィルス識別データファイルが前記処理クラスタに追加されたかに関する判断による関数である、請求項３５に記載の装置。

【請求項３７】

前記レスポンスの送信とは前記ファイルを送信することである請求項２１に記載の装置。

【請求項３８】

前記レスポンスの送信が、ユーザへの前記ファイルは利用不可能である旨の通知を含む請求項２１に記載の装置。

【請求項３９】

前記の、前記リクエストに対する応答が、前記ユーザに前記スキャンレポートの部分を送ることを含んでいる請求項２１に記載の装置。

【請求項４０】

クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、

サーバにおいてファイルに対するリクエストを受け取るステップ、

前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送るステップ、

前記ファイルをサーバから送信しても安全であるか否かについての指摘を前記スキャン装

置から受け取るステップ、および、
前記指摘が、前記ファイルの送信が安全であるとする場合、前記ファイルを送信することで前記リクエストに応答するステップを有する、クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項４１】
前記スキャン装置が、前記ファイルがいかなるウィルスにも感染していない場合に、前記ファイルを送信しても安全であると指摘する、請求項４０に記載の方法。
【請求項４２】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項４０に記載の方法。
【請求項４３】
前記サーバがウェブサーバである、請求項４０に記載の方法。
【請求項４４】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項４０に記載の方法。
【請求項４５】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項４４に記載の方法。
【請求項４６】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、
サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するステップ、
サーバにおいてファイルに対するリクエストを受け取るステップ、
データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するステップ、
および、
データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するステップを有する、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項４７】
データベースを保持するステップがさらに、
前記スキャン装置から受け取った指摘を追跡するステップ、および、
前記ファイルに対するアクセスを追跡するステップを有する、請求項４６に記載の方法。
【請求項４８】
前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項４７に記載の方法。
【請求項４９】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項４６に記載の方法。
【請求項５０】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項４６に記載の方法。
【請求項５１】
前記サーバがウェブサーバである、請求項４６に記載の方法。
【請求項５２】

クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法であって、
サーバより、前記サーバに接続されたスキャン装置において、前記サーバの大容量記憶装置に記憶されたファイルに対する識別子を受け取るステップ、
前記ファイルのウィルスをスキャンするステップ、および、
前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするステップを有する、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みる方法。
【請求項５３】
さらに、前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正するステップを有する請求項５２に記載の方法。
【請求項５４】
前記サーバがウェブサーバである、請求項５２に記載の方法。
【請求項５５】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項５２に記載の方法。
【請求項５６】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項５５に記載の方法。
【請求項５７】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバであって、
クライアント装置との通信リンク、
大容量記憶装置、
ならびに、
リクエストされたファイルをクライアント装置に送信するための命令を実行するプロセッサを有し、
前記命令が、
（ａ）ファイルに対するリクエストを受け取るための、
（ｂ）前記ファイルのウィルスをスキャンするスキャン装置に前記ファイルに対する識別子を送信するための、
（ｃ）前記ファイルをサーバより送信しても安全であるか否かについての指摘を前記スキャン装置から受け取るための、および、
（ｄ）前記指摘が、前記ファイルは送信しても安全であると指摘していれば、前記ファイルを送信することにより、前記リクエストに応答するための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバ。
【請求項５８】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記スキャン装置が、前記ファイルは送信しても安全であると示唆する、請求項５７に記載のサーバ。
【請求項５９】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項５７に記載のサーバ。
【請求項６０】
前記サーバがウェブサーバである、請求項５７に記載のサーバ。
【請求項６１】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項５７に記載のサーバ。
【請求項６２】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項

６１に記載のサーバ。
【請求項６３】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバであって、
クライアント装置との通信リンク、
大容量記憶装置、
ならびに、
リクエストされたファイルをクライアント装置に送信するための命令を実行するプロセッサを有し、
前記命令が、
（ａ）サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するための、
（ｂ）サーバにおいてファイルに対するリクエストを受け取るための、
（ｃ）データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するための、および、
（ｄ）データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるサーバ。
【請求項６４】
前記の、前記データベースを保持する命令がさらに、
前記スキャン装置から受け取った指摘を追跡するための、および、
前記ファイルに対するアクセスを追跡するための命令を有する、請求項６３に記載のサーバ。
【請求項６５】
前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項６４に記載のサーバ。
【請求項６６】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項６３に記載のサーバ。
【請求項６７】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項６３に記載のサーバ。
【請求項６８】
前記サーバがウェブサーバである、請求項６３に記載のサーバ。
【請求項６９】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるスキャン装置であって、
前記サーバとの通信リンク、および、
命令を実行するプロセッサを有し、
前記命令が、
（ａ）前記サーバの大容量記憶装置に記憶されたファイルに対する識別子をサーバより受け取るための、
（ｂ）前記ファイルのウィルスをスキャンするための、および、
（ｃ）前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするための、前記ファイルをサーバより送信しても安全であるか否かについての指摘を前記スキ

ャン装置から受け取るための命令をも含んでいる、
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるスキャン装置。
【請求項７０】
さらに、前記命令が、前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正する命令を有する請求項６９に記載のスキャン装置。
【請求項７１】
前記サーバがウェブサーバである、請求項６９に記載のスキャン装置。
【請求項７２】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項６９に記載のスキャン装置。
【請求項７３】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項７２に記載のスキャン装置。
【請求項７４】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、
前記命令が、
サーバにおいてファイルに対するリクエストを受け取るステップ、
前記ファイルのウィルスをスキャンするスキャン装置に、前記ファイルに対する識別子を送信するステップ、
前記ファイルをサーバから送信しても安全であるか否かについて、前記スキャン装置からの指摘を受け取るステップ、および、
前記指摘が、前記ファイルは送信しても安全であると指摘していれば、前記ファイルを送信することにより、前記リクエストに応答するステップを含んでいる、記憶装置。
【請求項７５】
前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記スキャン装置が、前記ファイルは送信しても安全であると示唆する、請求項７４に記載の記憶装置。
【請求項７６】
前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項７４に記載の記憶装置。
【請求項７７】
前記サーバがウェブサーバである、請求項７４に記載の記憶装置。
【請求項７８】
前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項７４に記載の記憶装置。
【請求項７９】
前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項７８に記載の記憶装置。
【請求項８０】
クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、
前記命令が、
サーバによって扱われているファイルが、サーバから送信しても安全であることを示唆するデータベースを保持するステップ、
サーバにおいてファイルに対するリクエストを受け取るステップ、
データベースが、前記ファイルは送信しても安全であると指摘するならば、前記ファイルを送信することによって前記リクエストに応答するステップ、および、

データベースが、前記ファイルは送信しても安全であると指摘しない場合に、前記ファイルに対する識別子を、前記ファイルのウィルスをスキャンするスキャン装置に送信し、前記ファイルはサーバから送信しても安全であるか否かについての指摘をスキャン装置から受け取り、かつ、前記指摘が、前記ファイルを送信しても安全であると指摘しているならば、前記ファイルを送信することで前記リクエストに応答するステップを含んでいる、記憶装置。

【請求項８１】

データベースを保持するステップがさらに、

前記スキャン装置から受け取った指摘を追跡するステップ、および、

前記ファイルに対するアクセスを追跡するステップを有する、請求項８０に記載の記憶装置。

【請求項８２】

前記ファイルが、前記追跡されている指摘が前記データベースに組み込まれて以降、変更されていれば、前記ファイルは送信しても安全であるという、前記データベースの前記追跡されている指摘はキャンセルされる、請求項８１に記載の記憶装置。

【請求項８３】

前記スキャン装置が、前記ファイルはいかなるウィルスにも感染していないと判断すれば、前記ファイルは送信しても安全であることを示唆する、請求項８０に記載の記憶装置。

【請求項８４】

前記リクエストをクライアント装置より受け取り、前記ファイルをクライアント装置へ送る、請求項８０に記載の記憶装置。

【請求項８５】

前記サーバがウェブサーバである、請求項８０に記載の記憶装置。

【請求項８６】

クライアントーサーバ環境においてウィルスからの保護を与えることを試みるための、プロセッサによって実行可能な命令を含んでいる情報を有する記憶装置であって、

前記命令が、

サーバより、前記サーバに接続されたスキャン装置において、前記サーバの大容量記憶装置に記憶されたファイルに対する識別子を受け取るステップ、

前記ファイルのウィルスをスキャンするステップ、および、

前記ファイルが感染しているか否かについて、前記サーバに指摘をレポートするステップを含んでいる、記憶装置。

【請求項８７】

前記命令がさらに、

前記ファイルのウィルスをスキャンした結果に基づいて、前記ファイルを変更、削除、または、さもなくば、修正するステップを有する請求項８６に記載の記憶装置。

【請求項８８】

前記サーバがウェブサーバである、請求項８６に記載の記憶装置。

【請求項８９】

前記スキャン装置は、前記スキャン装置同様に機能している前記サーバに接続されている装置のクラスタの１つである、請求項８６に記載の記憶装置。

【請求項９０】

前記装置のクラスタは、パーソナルコンピュータと相互接続したクラスタである、請求項８９に記載の記憶装置。

【発明の詳細な説明】

【発明の背景】

【０００１】

技術分野

本発明はネットワーク環境におけるウィルススキャンに関する。

【０００２】

関連技術

コンピュータネットワークおよびインターネットにより、エンドユーザはあらゆる種類の情報への国際的な共通基盤に基づく、新しいアクセスを享受している。情報へのアクセスは、電話線を用いてある種のコンピュータ装置をネットワークに接続するように簡便にできる。ワイヤレス通信の急増に伴い、今やユーザは事実上、どこからでもコンピュータネットワークにアクセスできる。

【０００３】

このような規模の接続性が、コンピュータウィルスの影響度を拡大している。「メリッサ(Melissa)」および「アイラブユー(I love you)」といったウィルスは、全世界のコンピュータシステムに壊滅的な打撃を与えた。ウィルス処置に要するコストはしばしば、数百万ドルにもまた数千万ドルにも達する。近年、ハンドヘルド型コンピュータ装置もまたウィルスに感染しやすいことがわかっている。

【０００４】

ウィルス保護ソフトウェアはウィルス対策において非常に効果的であり、またウィルス保護ソフトウェアはパーソナルコンピュータのような一般的なコンピュータ装置向けのものが広く流通している。しかしながら、ファイラ（データの記憶および検索に特化した装置）のような特殊なコンピュータ装置に固有の問題が存在する。市販のウィルス保護ソフトウェアは、特殊なコンピュータ装置上では、修正を加えない限り、実行されず、別のプラットフォームで稼動するようにソフトウェアを書き替えることは非常に高くつく。

【０００５】

第１の周知の方法はデータソースにおけるウィルススキャンである。特殊なコンピュータ装置によってデータが提供されようとすれば、その特殊なコンピュータ装置をスキャンする必要がある。装置内のファイルをスキャンするために、その装置用のウィルス保護ソフトウェアを記述しなければならない。

【０００６】

この第１の周知の方法は、ファイルに対してウィルススキャンをするには効果的な方法だが、幾つかの不利益を有する。先ず、特殊なコンピュータ装置を有する会社は、かなりの資産をかけてウィルス保護ソフトウェアを作りあげ、そして、現われる新しいウィルスから保護してくれるよう、データファイルを最新型に維持しなければならない。

【０００７】

そのうえ、特殊なコンピュータ装置の製造業者は、主流となっているウィルス保護ソフトウェアを作っている法人の賛助を得てカスタムアプリケーションを記述し、ライセンシーになることは可能だが、このことが、選択したアンチーウィルスソフトウェアベンダーの信頼性、ハードウェアがアップグレードされた場合の互換性に関する課題、および、多大な財務費用といった問題を引き起こしている。

【０００８】

第２の周知の、コンピュータウィルスから保護する方法は、エンドユーザに彼らのクライアント装置上でアンチーウィルスソフトウェアを実行させることである。アンチーウィルスソフトウェアは、マカフィー(McAfee)やシマンテック(Symantec)といった会社から提供されている。これらのプログラムはコンピュータのブート段階中にロードされ、バックグラウンドジョブとして動作してメモリおよびファイルを開いたり、保存したりしながら監視している。

【０００９】

この第２の周知の方法はクライアント装置の感染を阻止し、保護する上では効果的だが、幾つかの不利益を有する。これは連鎖における最終可能リンクに、検出の負担を設定している。いかなる理由があろうと、エンドユーザに到達するよりも先にウィルスを検出しなければ、ウィルスは最大の被害（ファイルの破壊、ならびに、他のコンピュータユーザおよびシステムへの拡大）を及ぼすであろうコンピュータ装置に到達する。

【００１０】

何百万というユーザへ送信されるかもしれないソースからファイルを駆除(sanitize)する

ほうが、そのファイルを送信し、そして、エンドユーザに、ファイルが感染している場合にそのファイルに対処するための用意をしておくことを期待するよりもずっとよい。エンドユーザはしばしば古いバージョンのアンチーウィルスソフトウェア、および／または、そのソフトウェアが新しく発見されたウィルスから確実に護れるようにするためのデータファイルにアップデートしていない。従って、大量配信されるポイントにおける検出を行うことがより重要である。

【００１１】

また、ハンドヘルド型コンピュータ装置もウィルスに感染しやすいが、これら装置のウィルスに対処する装備は不十分である。一般に、ハンドヘルド型コンピュータ装置はデスクトップシステムと比較して、非常に制限されたメモリリソースを有する。これらのリソースの一部分をウィルス保護に費やすと、ハンドヘルド型装置が効率的に動作する能力を厳しく制限する。情報ソースにおける信頼できるウィルススキャンが最も効率的でありかつ効果的な方法である。

【００１２】

ウィルスからの保護は絶え間の無い戦いである。新しいウィルスは毎日創出され、ウィルス保護ソフトウェア製造者は新しいデータファイル（アンチーウィルスソフトウェアが使用する解決用アルゴリズム）を作り出す必要に迫られる。ファイルのソースにおいて保護することで、ウィルスはさらに効率よく、効果的に除去可能である。

【００１３】

一般にデータのセキュリティーは重要である。同程度に重要なのがエンドユーザの信用である。これは会社に先行する評判に由来し、また、ウェブコマースに従事する会社は、その評判によって生きることも死ぬこともある。それは丁度、エンドユーザがウェブベースの売買取引のために開示したクレジットカードの番号が安全であると信じているように、受信するファイルも安全であることを望んでいる。

【００１４】

従い、特殊なコンピュータ装置をスキャンして、変更、削除、または、修正の必要があるかもしれない、ウィルスおよび他の悪質なもしくは望まざる内容を調べる技術を提供することが望まれている。

【発明の概要】

【００１５】

本発明は、（ファイラのような）特殊なコンピュータ装置に対してウィルススキャンする方法およびシステムを提供する。好適な実施形態においては、ファイラは１以上の補助的コンピュータ装置と接続されており、この補助的コンピュータ装置がエンドユーザへの送信の前に、要求されたファイルをスキャンしてウィルスフリーであることを確かめる。エンドユーザがファイラからファイルを要求すると、以下のステップが実施される。第１に、要求されたファイルはエンドユーザに向けて送信する前にスキャンされなければならないかどうかを判断する。第２に、ファイラは外部コンピュータ装置の１つへのチャンネルを開き、ファイル名を送る。第３に、その外部コンピュータ装置がそのファイルを開いてスキャンする。第４に、外部コンピュータ装置がファイラへファイルスキャン操作のステータスを報告する。第５に、ファイラは、前記ステータスが送信してもよいことを示せば、ファイルをエンドユーザに送る。

【００１６】

本システムは、ファイルが修正されるか、または、新しいウィルスから保護するための新しいデータファイルが付加されないかぎり、たった一度だけファイルをウィルススキャンする必要があるという点で、非常に効率的でありまた効果的である。スキャンしたファイルのスキャンレポートは、１以上の外部コンピューク装置、１以上のファイラに記憶されてもよく、そして、スキャンレポートのある部分はエンドユーザに送信されてもよい。

【００１７】

本発明の代替的実施形態においては、１以上のコンピュータ装置が、ファイルの圧縮や暗号化といった他の補助的アプリケーションを独立に、または、組み合わせて、実行してい

てもよい。

【好適な実施形態の詳細な説明】

【００１８】

以下の説明にて、本発明の好適な実施形態を、その好適な処理工程およびデータ構造に着目し、説明する。当業者であれば本出願を精読した後には、本発明の実施形態は１以上の一般目的もしくは特殊目的プロセッサ、または、他の、本明細書に記載の特定の処理工程およびデータ構造に適合した回路を用いて実施可能であること、ならびに、必要以上の試験または更なる発明を必要とせずに本明細書に記載の処理工程およびデータ構造を実施することができることを理解するであろう。

【００１９】

辞書編集(Lexicography)

以下の用語は、以下に説明する本発明の態様を、言及または関連する。これら用語に関する一般的な意味についての記載は、制限を加えることを目的としたものではなく、単に例示目的にすぎない。

・ウィルス－一般的に、人間が作り出したプログラムまたはコードの断片であって、コンピュータユーザの認識なしに、そのコンピュータにロードされ、そして、ユーザの意に反して実行される。たいていのウィルスは自己複製可能であり、さらに危険なタイプのウィルスにあってはネットワークを介して自身を送信し、セキュリティーシステムを迂回する能力を有する。

・クライアントおよびサーバ－一般的に、これら用語は２つの装置間の関係性について述べている。特に、クライアントおよびサーバという関係性を述べる上で必ずしも特定の物理的な装置を必要としない。

例えば、これに制限されないが、第１サーバ装置と第１の関係性を有する特定のクライアント装置が、第２クライアント装置と第２の関係性を有してサーバ装置として機能することが可能である。好適な実施形態においては一般に、比較的少数のサーバ装置が比較的多数のクライアント装置に対して情報提供を行う。

・クライアント装置およびサーバ装置－一般に、これら用語は、（ＨＴＴＰウェブクライアントおよびウェブサーバのように）クライアントーサーバ関係においてクライアント装置またはサーバ装置の役割を果たす装置をいう。いかなるクライアント装置またはサーバ装置も個別的な物理的装置でなければならないという特別な要求はない。これらは単一の装置であっても、協働する装置群であっても、装置の部分であっても、または、それらのうちのある組み合わせであってもよい。

例えば、これに制限されないが、クライアントーサーバ関係におけるクライアント装置およびサーバ装置は、実際には物理的に同一の装置とすることが可能であり、第１ソフトウェア要素群によりクライアント機能が発揮され、第２ソフトウェア要素群によりサーバ機能が発揮される。

・ウェブクライアントおよびウェブサーバ（もしくはウェブサイト）－本明細書中にて用いられる用語「ウェブクライアント」および「ウェブサーバ」（もしくは「ウェブクライアント」）は、インターネット、ワールドワイドウェブ、または、その均等物もしくはその拡張物におけるクライアントーサーバ環境において、ウェブクライアントまたはウェブサーバの役割を果たす、あらゆる装置の組み合わせまたはソフトウェアをいう。ウェブクライアントが個別的な装置でなければならないという特別な要求はない。これらは単一の装置であっても、協働する装置群であっても、装置の部分であっても、または、それらのうちのある組み合わせであってもよい（たとえば、ウェブサーバ機能を有する装置がユーザのエージェントとして動作しているように）。

【００２０】

上述のように、これらの用語に関する一般的な意味についての説明は、それらに限定することを意図したものではなく、例示を目的としている。本発明の他の、そして、さらなる適用は、これらの用語および概念の拡張も含まれているが、本出願を精読した後には、当業者にとっては明瞭であろう。これらの他の、そして、さらなる適用は本発明の範囲およ

び本発明の思想の一部であり、それらは当業者であれば別の発明または必要以上の試験をせずとも明らかである。

【００２１】

システムの要素

図１は分散化装置によるウィルススキャンのためのシステムに関するブロック図を示す。

【００２２】

システム１００はユーザ１１１と関連するクライアント装置１１０、通信ネットワーク１２０、ファイラ１３０、および、処理クラスタ１４０を有する。

【００２３】

クライアント装置１１０はプロセッサ、主メモリ、および、命令を実行するためのソフトウェア（図示せず、だが当業者であれば理解する。）を有する。クライアント装置１１０およびファイラ１３０は別個の装置として示されるが、これらが物理的に分離していることを要求しない。

【００２４】

好適な実施形態において、通信ネットワーク１２０はインターネットを含む。代替的実施形態において、通信ネットワーク１２０は、イントラネット、エクストラネット、仮想プライベートネットワーク、ダイレクト通信リンク、または、それらの組み合わせもしくは結合といった、代替的通信形態を含んでもよい。

【００２５】

通信リンク１１５はクライアント装置１１０と通信ネットワーク１２０を接続している。

【００２６】

ファイラ１３０はプロセッサ、主メモリ、命令を実行するためのソフトウェア（図示せず、だが当業者であれば理解する。）、および、大容量記憶装置１３１を有する。クライアント装置１１０およびファイラ１３０は個別の装置として示されているが、これらが個別的な装置である必要性はない。ファイラ１３０は通信ネットワーク１２０に接続されている。

【００２７】

大容量記憶装置１３１は、クライアント装置１１０からリクエスト可能な、少なくとも１つのファイル１３３を有する。

【００２８】

処理クラスタ１４０は、１以上のクラスタ装置１４１を有し、クラスタ装置１４１それぞれはプロセッサ、主メモリ、命令を実行するためのソフトウェア、および、大容量記憶装置（図示せず、だが当業者であれば理解する。）を備えている。ファイラ１３０および処理クラスタ１４０は個別の装置として示されているが、これらが個別的な装置である必要性はない。

【００２９】

好適な実施形態においては、処理クラスタ１４０は、相互通信およびファイラ１３０との直接通信可能な相互接続クラスタにおける複数のパーソナルコンピュータである。

【００３０】

クラスタリンク１３５は、処理クラスタ１４０とファイラ１３０とを接続する。クラスタリンク１３５は不均等メモリアクセス、または、イントラネット、エクストラネット、仮想プライベートネットワーク、ダイレクト通信リンク、または、それらの組み合わせもしくは結合による通信を含んでいてもよい。

【００３１】

操作方法

図２は分散化装置のウィルススキャンのためのシステムの処理流れ図である。

【００３２】

方法２００は、一組の流れのポイントおよび一組のステップを有する。システム１００が方法２００を実施する。方法２００は連続的に説明されているが、個々の要素は連動的または並列的に、非同期的にパイプライン方式で、また、その他の方式で、方法２００のス

テップを実施可能である。方法２００は、そのように指示されている場合を除き、本明細書に羅列したステップの順番と同一の順番で実施される必要性を有しない。

【００３３】

流れのポイント２００において、システム１００は方法２００を実施開始する用意ができている。

【００３４】

ステップ２０１において、ユーザ１１１はクライアント装置１１０を利用し、ファイル１３３に対するリクエストを開始する。リクエストは通信ネットワーク１２０を介してファイラ１３０に送信される。好適な実施形態においては、ファイラ１３０はウェブサーバ（図示せず、だが当業者であれば理解する。）の指示でファイル検索および記憶を実行する。

【００３５】

ステップ２０３において、ファイラ１３０はファイル１３３に対するリクエストを受け、ファイルＩＤおよびファイル１３３のパスを処理クラスタ１４０へ送信し、処理クラスタにおいて、クラスタ装置１４１のうちの１つがそれを受信する。

【００３６】

ステップ２０５において、クラスタ装置１４１はファイルＩＤおよびパスを利用してファイラ１３０の大容量記憶装置１３１のファイル１３３を開く。

【００３７】

ステップ２０７において、クラスタ装置１４１はファイル１３３のウィルススキャンを行う。好適な実施形態においては、ファイルは総当り方式(round robin fashion)で処理クラスタに課せられる(be tasked to the processing cluster 140)。代替的実施形態において、ファイルはクラスタ装置１４１によって個別的に処理されてもよく、複数のクラスタ装置１４１によって同時的にされてもよく、また、それらの組み合わせでもよい。処理クラスタ１４０内における処理の最大効率化を確保する目的で、負荷分散(load balancing)を用いてもよい。

【００３８】

パーソナルコンピュータ向けのウィルス保護ソフトを提供するベンダーは数社あるので、ファイラ１３０の操作者は使用したい製品なら何でも選んでよい。また、処理クラスタ１４０において複数ベンダーの製品を組み合わせて使用することすらかまわない。本発明の代替的実施形態においては、ファイラ１３０のあらゆるファイル１３３に対して継続的にスキャンが行われてもよい。

【００３９】

処理クラスタ１４０は高度な拡張性を有する。パーソナルコンピュータの価格は、ファイラのような専用の装置に較べて低価格であるので、このような構成は非常に望ましいものである。加えて、クラスタの構成により、クラスタ装置１４１が機能停止した場合における代理機能システム(redundant systems)を提供し、処理クラスタ内部においてフェイルオーバー(failover)およびテイクオーバー(takeover)も可能である。

【００４０】

ステップ２０９において、クラスタ装置１４１はスキャンリポートをファイラ１３０に送信する。スキャンリポートは主としてファイルが送信しても安全であるかについて報告する。別の情報についても、データベースに統計上の目的で保存してもよい（例えば、どれくらいのファイルが感染していると特定されたか、ウィルスソフトウェアはそのファイルを駆除(sanitize)できたか、または、ファイルは削除されたか）。続いて受信されたリクエストに基づく送信に際し、その前にファイル１３３をスキャンする必要があるかどうかを、前記データベースを参考にして決定してもよい。ファイル１３３が、最後にスキャンを受けて以来、変更を受けておらず、かつ、さらなるウィルスデータファイルが処理クラスタに付加されていなければ、ファイル１３３は、おそらくスキャンを受ける必要はない。つまり、ファイル１３３はさらに迅速に送信可能である。

【００４１】

他の中間的アプリケーションも、処理クラスタ１４０内において独立して実行しても、他のアプリケーションと結合して実行しても、または、その組み合わせとして実行してもよい。圧縮および暗号化ユーティリティはこれらアプリケーションの例である。ウィルススキャンを含むこれらのアプリケーションは、非常にＣＰＵに負担をかけるものであり、したがってアウトソーシングによりファイラのような専用の装置が最もすべきことを実行し、他のタスクは処理クラスタ１４１に請け負わせることが可能となり、よりよいパフォーマンスをもたらす。

【００４２】

ステップ２１１において、ファイラ１３０は、処理クラスタ１４０によるスキャンを受けて報告される利用可能性に基づいてファイル１３３をクライアント１１０に向けて送信する、または、送信しない。スキャンレポートのある部分については、ユーザへ送信してもよい。

【００４３】

本ステップにおいて、ファイル１３３に対するリクエストは受信されており、前記リクエストは処理され、そして、可能であるのならばファイル１３３は配信される。本処理は後のリクエストに対して、ステップ２０１から繰り返されてよい。

【００４４】

本発明の一般性

本発明は、ファイルに対する処理要求の別の態様に対して広範な利用可能性および一般性を有する。

【００４５】

本発明は、１以上の、以下を含むような環境に、または、それらの組み合わせに対して利用可能である。

・ファイル圧縮

・ファイル暗号化、および、

・ＣＰＵに負担をかけるタスクを専用装置から多目的コンピュータへ委託する、一般的なアウトソーシング。

【００４６】

代替的実施形態

本明細書において好適な実施形態について開示したが、本発明の概念、範囲、および、思想の範囲内においてさまざまな変形例が可能である。これらの変形例は、本出願を精読の後には当業者にとって明白である。

【図面の簡単な説明】

【００４７】

【図１】分散化された装置でのウィルススキャンのためのシステムのブロック図である。

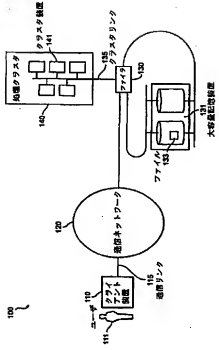
【図２】分散的ウィルススキャンのためのシステムの処理の流れ図である。

【符号の説明】

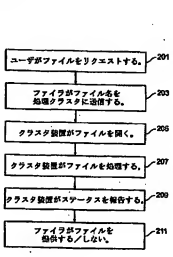
【００４８】

１００　・・　システム　　１１０　・・　クライアント装置
１１１　・・　ユーザ　　１１５　・・　通信リンク
１２０　・・　通信ネットワーク　　１３０　・・　ファイラ
１３１　・・　大容量記憶装置　　１３３　・・　ファイル
１３５　・・　クラスタリンク　　１４０　・・　処理クラスタ
１４１　・・　クラスタ装置

【図１】


クラスタ装置
141
クラスタクリンク
135
処理クラスタ
ファイバ
130
140
131
大容量記憶装置
ファイバ
133
通信ネットワーク
120
ファイバ
115
通信リンク
クライアント装置
110
ユーザ
111
100

【図２】


200
ユーザがファイルをリクエストする。
201
ファイラがファイル名を処理クラスタに送信する。
203
クラスタ装置がファイルを開く。
205
クラスタ装置がファイルを処理する。
207
クラスタ装置がステータスを報告する。
209
ファイラがファイルを自分する／しない。
211